Securden

Endpoint Privilege Manager (EPM)

End User Guide

For Windows Users

Index

Securden Endpoint Privilege Manager

End User Guide – For Windows Users

Introduction

This document is designed to be used by standard users on Windows machines for gaining access to applications, elevate applications, and gain temporary admin rights using the Securden Endpoint Privilege Manager.

Note: This document is not relevant for users who are local administrators on their machines, or if Securden's application control measures are not enforced.

How can Windows Users Use the Securden Agent?

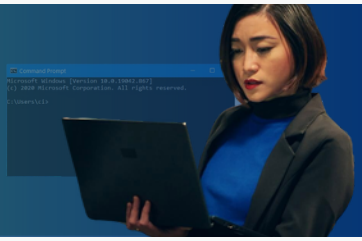
End Users can make use of the endpoint privilege manager to raise requests to gain permissions to run specific applications with admin rights, gain temporary admin rights, elevate the privileges of an application by leveraging permissions granted through policies.

Apart from privilege elevation, end users who are denied access to certain applications through allowlists and blocklists can raise a request to gain temporary access to those applications.

All these are handled through the Securden Agent and the steps to be followed for each scenario are explained in the sections below.

1. How to Run Applications with Admin Rights?
2. How to Raise a Request for Elevating an Application?
3. How to Raise a Request for Temporary Local Admin Rights?
4. How to Raise a Request for Temporary Access to Applications?
5. How to Elevate Applications and Gain Temporary Admin Rights when Offline?

How to Run Applications with Admin Rights?



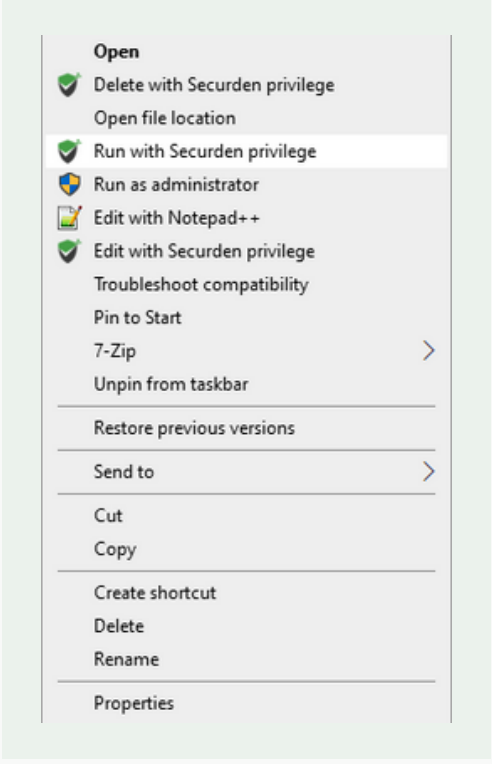
When you are working with an account with standard user rights, you can make use of the Securden Agent to run the application with admin rights. You can try to elevate an application by any of the following methods.

1. Run with Securden Privilege
2. Using the Command Prompt
3. Using the UAC prompt
4. Double-clicking the application

Option 1 : Running an Application with Securden Privilege

You can try to elevate any application that might normally need admin rights to run by right-clicking on the desired application.

If the Securden agent is installed on the machine, the context menu would have the option named **Run with Securden Privilege.**

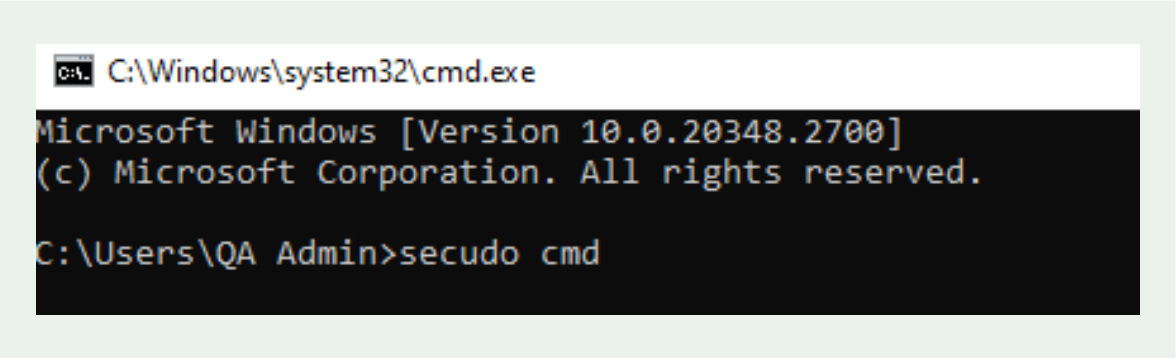


Selecting this option will launch the application with admin rights if the user has the required permissions to elevate the application.

Note: this option is not available for Start menu executables.

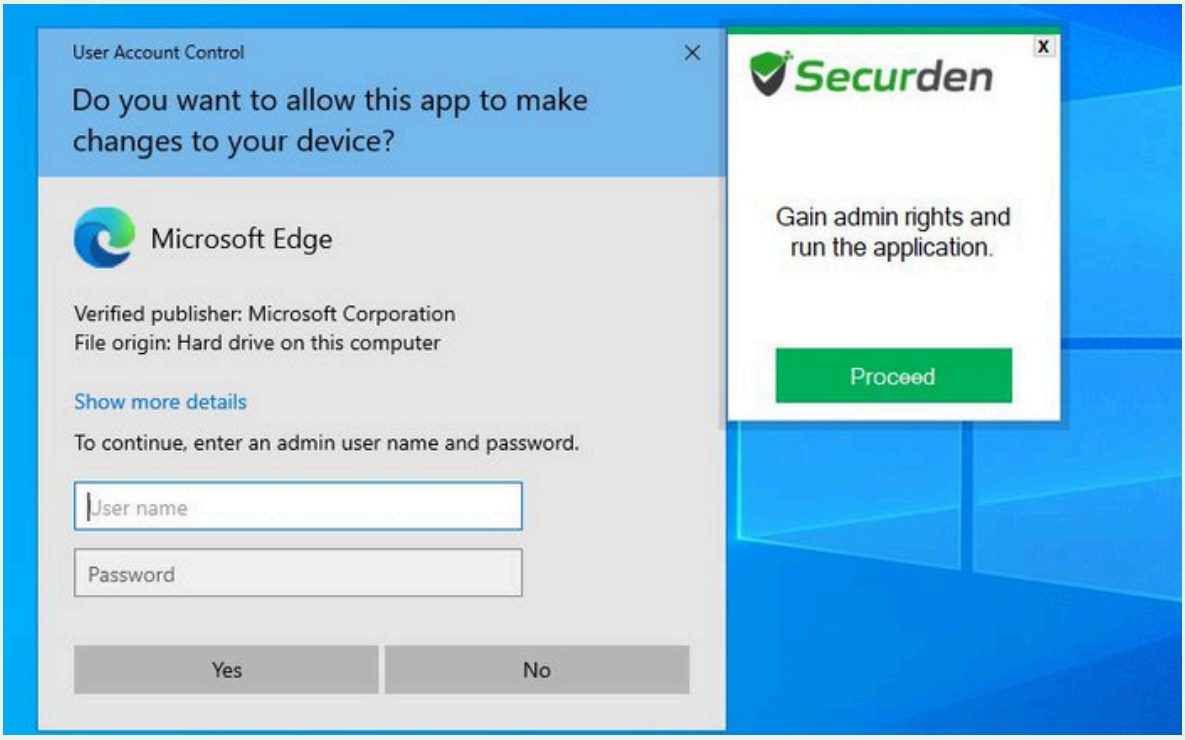
Option 2 : Using the Command Prompt to Elevate Applications

Securden provides the users with the option to use the command prompt and the run command to elevate applications. All the users have to do is append the prefix secudo to the application name.
For example, *secudo powershell*



Option 3 : Elevating Using the UAC Prompt

In cases where running an application will trigger the UAC prompt for authentication, the Securden agent will display a prompt alongside the UAC prompt. This prompt can be used to elevate the application.



If you have a policy that allows you to run the specific app with admin rights, you can click **Proceed** in the Securden popup adjacent to the UAC prompt.

The Securden Agent will take care of filling up the UAC prompt and elevate the application for you.

This method is particularly useful for running Control Panel items and start menu executables that might need admin rights for running.

Option 4 : Double Clicking the Application

This option is not available by default. If you want, you can request your administrator for the same.

If this option is enabled, you can access the application just like usual, by double-clicking the application file.

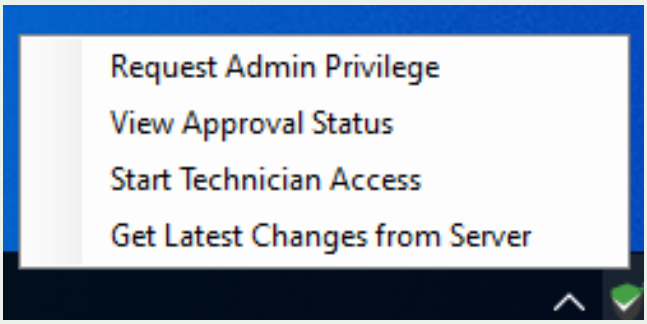
All the above options will only work if you have the required permission for elevating the privileges for the specific application. Permission to elevate applications can be obtained through control policies or by raising requests with the administrator.

How to Raise a Request for Elevating an Application?

You can raise a request for elevating an application in two ways. The first one is to use the Securden Agent tray icon, and the second method is to try and elevate an application for which you do not have the required permissions granted through policies.

Option 1 : Steps for Raising a Request from the Securden Agent Tray Icon

1. Click on the tray icon and choose Request Admin Privilege.



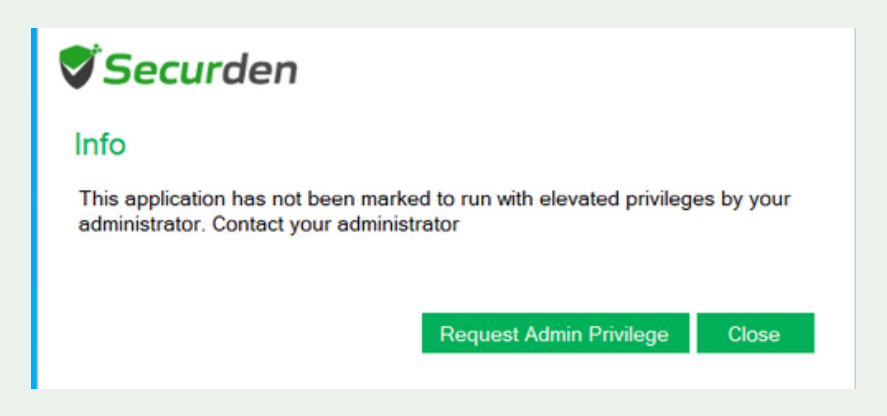
2. In the window that opens, select the option named For a specific application.
3. Click on Browse an application to select the required application.
4. Specify the time till when you would need to run the app with admin rights.
5. Provide a suitable reason for your administrator and click Request to raise the request.

Note: If an allowlist/blocklist policy is enforced, you will see a checkbox named With Admin Rights. You need to select this checkbox before placing the request.

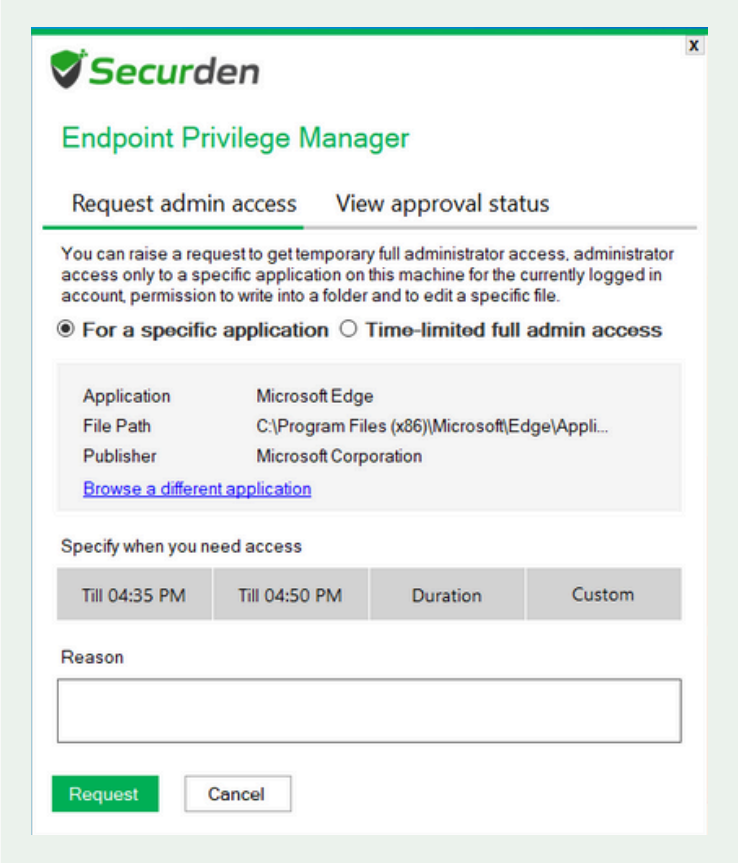
Option 2 : Steps for Raising a Request by Attempting to Elevate the Required Application

1. Use any of the methods discussed in the previous section “How to Run Applications with Admin Rights” to try to elevate the required application.

2. A popup will be displayed stating that you do not possess the permissions required to elevate the application. In this popup, you will have the option to request admin privilege.

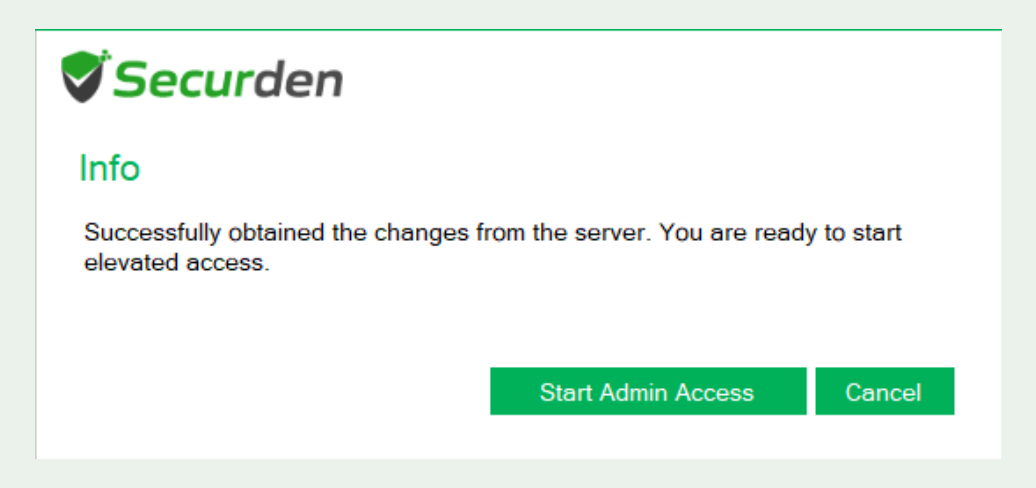


3. You need to specify the end time of the elevated access and provide a reason before raising the request.



Note: If an allowlist/blocklist policy is enforced, you will see a checkbox named **With Admin Rights.** You need to select this checkbox before placing the request.

Once the request is approved, you will receive a notification through email and via the agent. You can then elevate the application by clicking on **Start Admin Access.**



Note: Once the elevated application access begins, a timer will be displayed in the bottom right corner. This is the time left until you can run the app with admin rights. Once it runs out, the application will be terminated, and admin access will be automatically revoked.

How to Raise a Request for Time-limited Local Admin Rights?

In the last section, the steps involved in raising a privilege elevation request for a specific application. If you need to install multiple applications or elevate multiple applications at the same time, gaining temporary admin rights is the most efficient way to avoid waiting for multiple requests to get approved.

You can request temporary admin rights from the web-interface using the self-service portal or use the Securden Agent tray icon.

Option 1 : Using the Self-service Portal to Raise a Request for Temporary Local Admin Rights

1. Login to the Securden web interface to access the self-service portal.

2. Here, you will have the option to choose the device on which you want to get temporary local admin rights.

3. You can place the request for immediate use by selecting Now for the Request From option. If you want to raise a request for future use, you need to select the option Specify.

4. If you are placing a request for immediate use, you need to provide the appropriate end time of admin access. Specify this value with respect to the server time displayed in the portal.

5. If you are raising a request for a later time, you need to provide the start and end time according to the server time displayed in the portal.

6. You can view the approval status of your request on the right-hand side of the self-service portal.

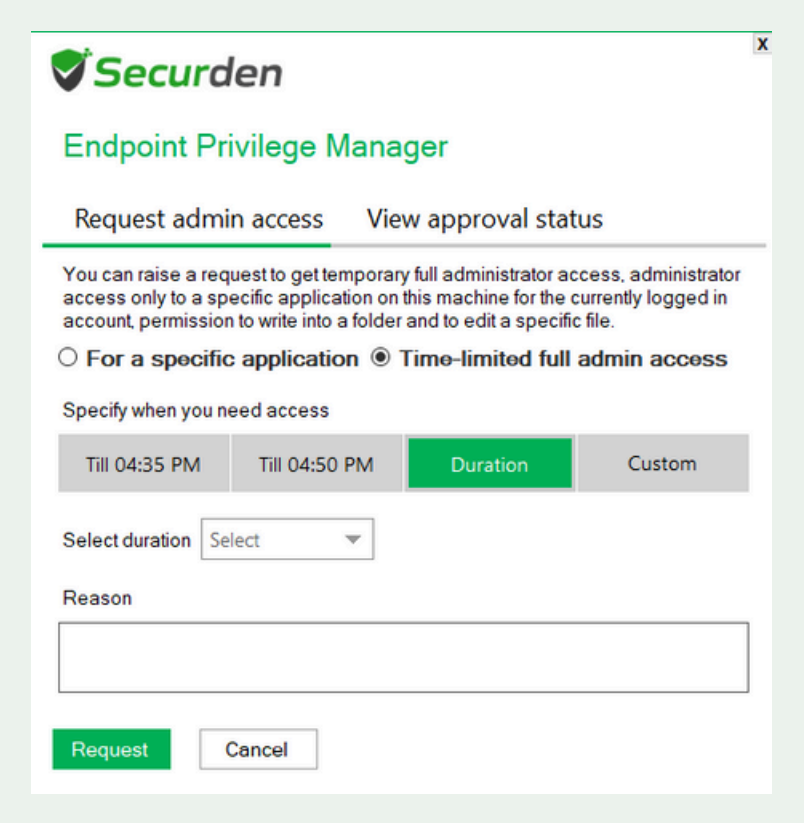
Once the request is approved, you can start admin access according to the start time of access and complete your task.

The elevated access time left is displayed by the agent in the bottom right corner of the screen. Once this timer runs out, all open tabs will be terminated, and admin rights will be revoked. Plan accordingly.

Option 2 : Using the Securden Tray Icon to Raise a Request for Temporary Admin Rights?

1. Click on the Securden Agent Tray icon and select **Request Admin Privilege.**

2. Select the radio button named **Temporary Full Admin Access.**



3. Specify the start and end time or the duration of elevated access you need.

4. Provide a suitable reason for justifying the request to your administrator before clicking **Request**.

Once the request is submitted, you need to wait for approval. Once you get the approval, you can start using the elevated access according to the time granted by the admin.

Note: Once temporary admin access begins, a timer will be displayed in the bottom right corner. This is the time left for admin access. Once it runs out, all active windows will be terminated, and admin access will be automatically revoked.

How to Raise a Request for Temporary Application Access?

When the administrator has enforced allowlists or blocklists for application control, you (end user) will not be able to run every application on your endpoint. If you need to access an application to which you do not have access currently, you can raise a request for temporary application access.

Note: Temporary application access will only allow you to run the application with the same privileges associated with the user account. This will not elevate the application privileges.

You can raise a request for temporary application access in two ways.

1. Using the Securden Agent Tray icon.
2. Using the Securden pop-up when attempting to access the app.

How to place the request using the tray icon?

Follow the steps below to raise a request for temporary application access using the **tray icon.**

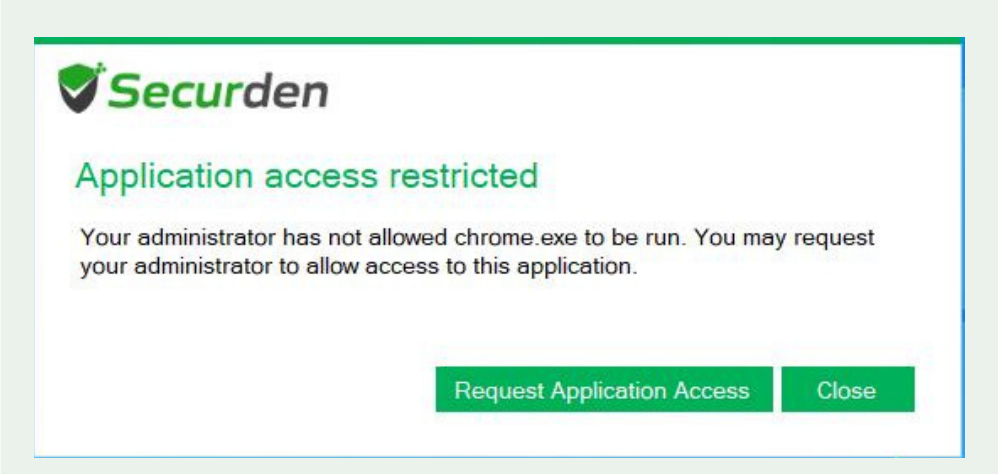
1. Click on the tray icon and select Request Application Access.
2. When raising an application access request, you will have two options. You can request access to a specific application or for all applications.
3. If you need to run multiple applications outside the list of allowed apps, you can select the latter option. However, this will temporarily disable the allowlist/blocklist.
4. If you are raising a request for a specific application, you need to browse your computer and select the required app.
5. Now, you need to specify the start and end time of application access. You have a few options here.

- You can select the end time and start access right after the admin approves the request.
- You can specify the start and end time and place the request.
- You can specify a duration (eg. 5 mins, 10 mins) and start whenever you need access. Once the admin approves, the permission stays active for a limited time. You need to start application access before expiry.

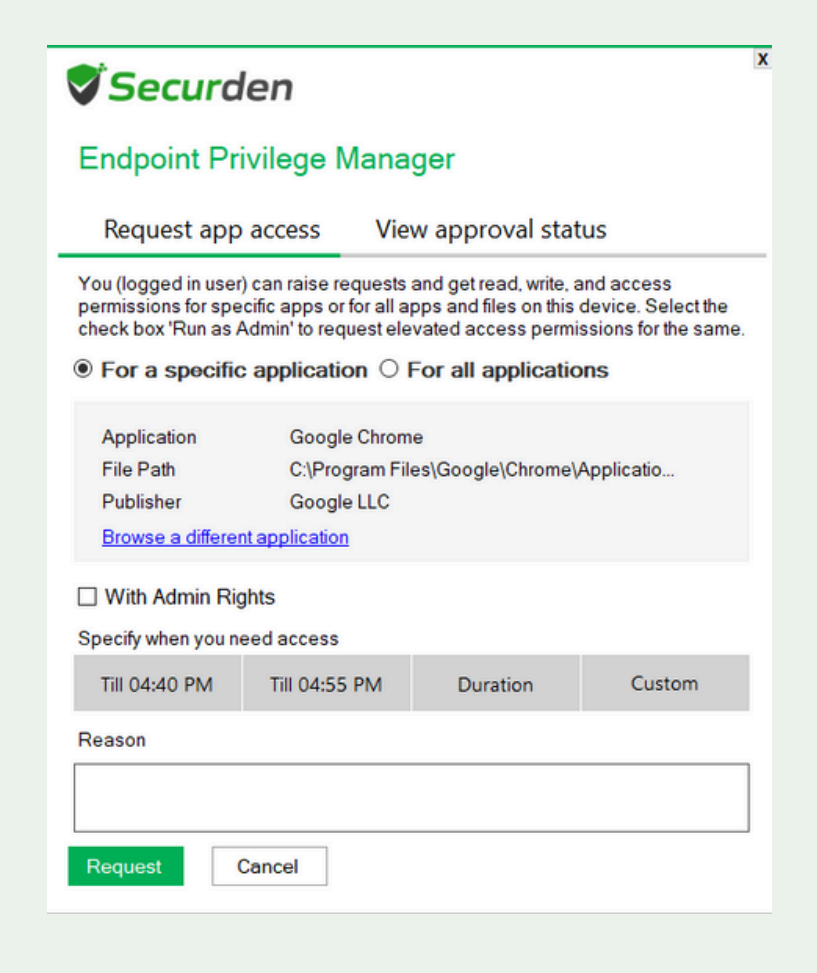
6. Once the time parameters are defined, you need to specify a reason before placing the request.

If you want to place the request by directly attempting to access an application, follow the steps below.

1. When an attempt to access an app without having permissions, a pop-up will be displayed with the option to place a request with the administrator. Click on **Request Application Access** to place a request.



2. Specify the time or duration of application access according to your specific need.



3. Provide a reason and click **Request**.

Note: If you want to run the application with admin rights, you need to select the checkbox named **With Admin Rights** before placing the request.

How to Gain Temporary Access when Offline?

Users connecting remotely might sometime need to run applications with admin rights. The Securden agent will enforce the latest control policies even when offline. If the application is part of a policy that allows you to elevate the application, then you can run the application with admin rights.

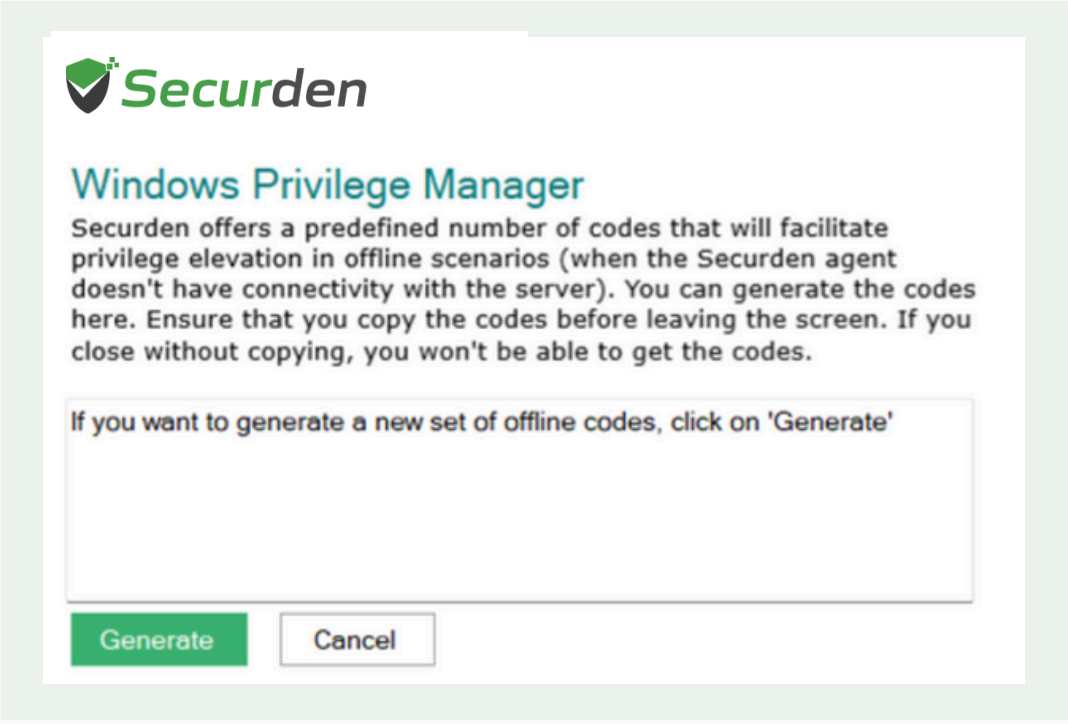
In certain cases where you need to elevate apps that are not a part of a policy, or if you need to access a blocklisted application, or if you need to gain temporary local admin rights when offline, you can make use of the offline access provisions in Securden.

Securden provides a provision to generate offline access codes that can be used to elevate application privileges or gain temporary admin rights. Offline access codes can be generated in two ways. The admin can generate offline access codes for you or you yourself can generate a set of offline access codes.

How to generate offline access codes?

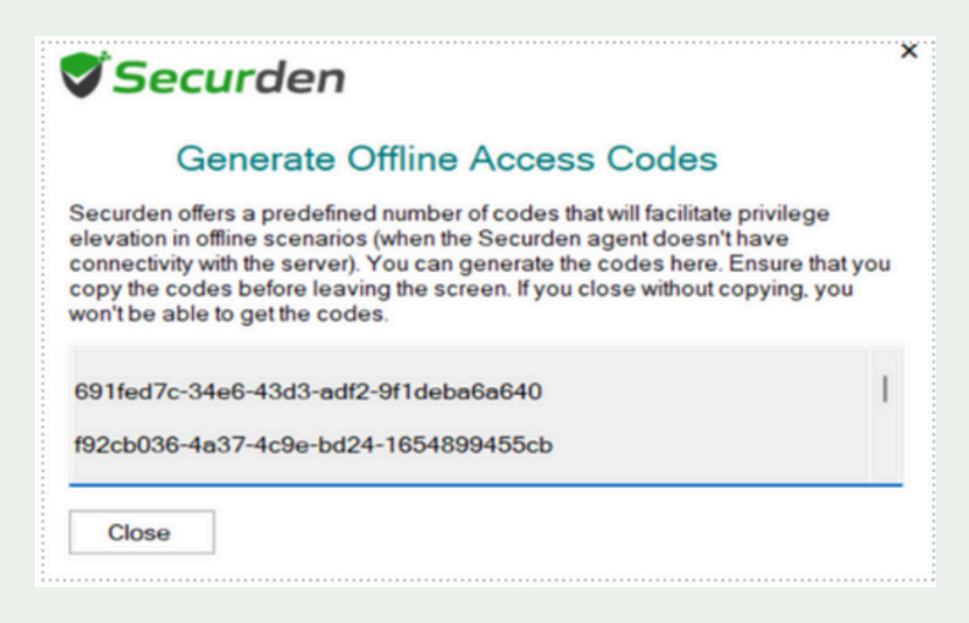
When the agent on your endpoint is still connected to the EPM server, you can generate a set of offline access codes from the Securden Agent tray icon.

1. Click on the agent tray icon and select **Generate Offline Access Codes.**
2. In the window that opens, click **Generate**.



Note: Generation of offline access codes by users must be allowed by the administrator for you to be able to generate codes.

Once the codes are generated, you need to save a copy of the codes in a secure file.



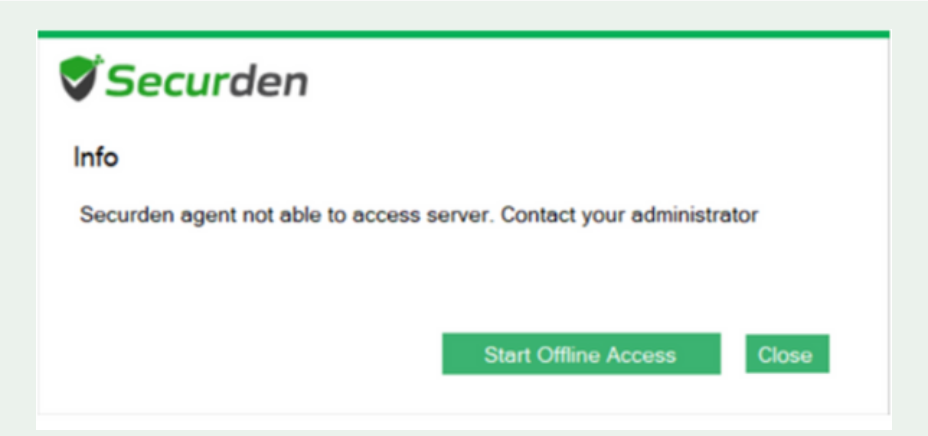
If you have lost the generated offline codes, you have to regenerate the codes once again. Your administrator must allow offline code regeneration from the web interface for you to be able to regenerate the codes.

How to use offline access codes?

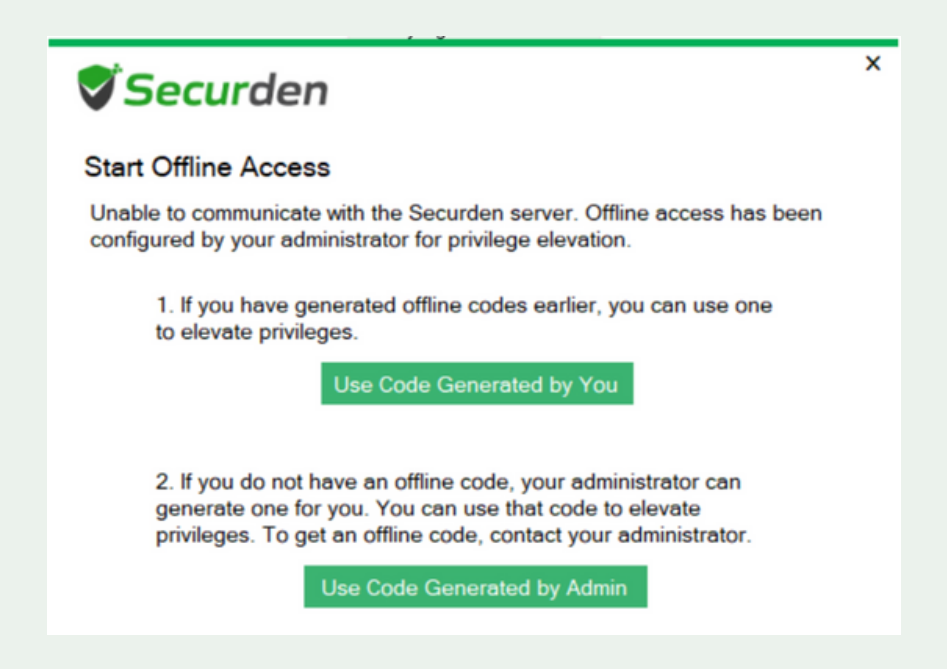
You can use the offline access codes you generated previously or make use of the codes shared by your administrator to elevate privileges when offline. You can proceed with the usual steps you would follow to elevate an application or gain temporary admin access.

An agent pop-up will be displayed stating that you do not have connectivity with the server to raise a request. The pop-up will have the option to use an offline access code.

1. Click **Start Offline Access.**



2. In the window that opens, you will be shown either one or both options (in image) based on the configurations made by your administrator.



3. If you have previously generated offline codes, you can choose the corresponding option. If you do not have any such code, you need to contact your admin for generating offline codes for you and share the code with you.

4. You can use one offline code to perform one privilege elevation activity.

Note: If you tried to gain temporary admin rights, you will be allowed to use the offline code only if the administrator has permitted the use of offline codes to gain full admin access.

For elevating applications, the agent would first check the policies for permission to elevate the application. If you do not have a policy that allows you to elevate the application, you will be asked to provide an offline access code to elevate the application.